



Let's build a smarter planet



MoneyGram International

Detects and prevents money transfer fraud before it impacts customers

Smart is...

Optimizing decision making processes to mitigate fraud and safeguard business

Using a powerful algorithms-based software platform, MoneyGram International managers can better understand who is using the company's services—knowledge that has helped them prevent more than US\$37.7 million in fraudulent transactions, reduce customer fraud complaints by 72 percent and quickly address regulatory requirements. The solution helps integrate information in real-time and provides actionable insight so company managers can quickly identify questionable patterns and proactively enact new processing rules to reduce fraud.

Ted Bridenstine, systems development manager at MoneyGram—a leading global payment services company—underscores the importance of fraud detection with the story of a 100-year old grandmother who had contacted MoneyGram after receiving a call that her grandson had been arrested and needed US\$2,500 for bail.

Behind the scenes, MoneyGram's fraud detection system flagged the transaction as suspicious. Analysts determined that it was likely part of a telephone scam and a MoneyGram representative contacted the customer to let her know that the wire had been stopped and her money was being refunded. Worried about her grandson's safety, she threatened to take her business elsewhere if MoneyGram didn't wire the money. The company representative implored the woman to contact a family member and verify the story.

"She called back three days later in tears to thank the representative personally," recalls Bridenstine. "She did verify that it was a fraud. She lives on Social Security and could not afford to lose money. The call was emotional and heartwarming."

With 230,000 locations in 190 countries and territories, MoneyGram has always had a robust fraud and anti-money laundering (AML) program. However, the company's IT staff found that the existing infrastructure wasn't flexible enough to keep up with rapidly changing compliance regulations and constantly evolving fraud tactics. In the past, new "rules"





Business benefits

- Increased ability to identify and interrupt potentially fraudulent transactions by 40 percent
 - Prevented thousands of customers from losing funds to fraud
 - Stopped more than US\$37.7 million in fraud
 - Realized a 72 percent reduction in consumer fraud complaints in one year
-

to trap fraudulent behavior had to be hard-coded into legacy mainframe and middleware applications. It was a time-consuming and complex process that could take weeks or months to complete.

Additionally, because of the nature of MoneyGram's business, there is no single data element that associates an individual with one or more transactions as that individual interacts with the system. As a result, it was extremely difficult for analysts to identify overall how much each customer wired during a specified time period—and this was a key requirement of the European Union's Payment Services Directive of 2009.

“Because we had a transaction-centric model, there were no specific customer identifiers,” says Bridenstine. “This made aggregating transaction activity based on the individual customer a huge problem for us with the passage of the Payment Services Directive.”

Building a platform for success

MoneyGram is becoming an analytics-driven organization by transforming its operations to obtain a clear view of its customers and confidently predict and prevent fraudulent behavior. This work includes creating a single engine for managing the rules by country or group of countries, and within high-volume transaction corridors.

“There are multiple layers of regulations—states, countries, the European Union, all layered upon each other,” explains Bridenstine. “We need the flexibility to collect customer data by geography and identify who our customers really are. For example, if a customer in Spain wired more than €3,000 in a three-month period, we needed to be able to flag that transaction and request more information from the client.”

Smarter Detection: Mitigating risk through sophisticated transaction analysis



Instrumented

Draws on transactions initiated through a broad range of banking systems throughout the world



Interconnected

Supports an end-to-end process for scanning all transactions and confirming their legitimacy before approving them



Intelligent

Scans thousands of daily transactions, marking suspicious or high-risk transactions based on established criteria to identify potentially fraudulent activity



Solution components:

Software

- IBM® InfoSphere® Identity Insight solutions
 - IBM Anonymous Resolution
 - IBM InfoSphere Global Name Recognition
 - IBM InfoSphere Identity Insight
- IBM InfoSphere Information Server
 - IBM InfoSphere DataStage®

IBM Business Partner

- Alpine Consulting, Inc.
-

“We are able to detect and respond to fraud far faster than before to protect our consumers as well as our global network of agents. We must remain ever vigilant in the face of more sophisticated financial fraudsters.”

— Ted Bridenstine, Systems Development Manager, MoneyGram International

And all of these processes have to happen without impacting customer service. “We count milliseconds in our transaction stream,” says Bridenstine. “There are a lot of activities that happen in transferring money and to add another step in the transaction flow was a concern.”

Protecting its customers

Working with IBM and Alpine Consulting, MoneyGram has gained clear visibility into the transaction history of each customer and insight into “who’s who?”, “who knows whom?”, and “who does what?” as it analyzes money transfers. The company’s new fraud prevention system (known as the Global Compliance project during implementation) helps stop fraud in its tracks and reduces the overall time and work required to respond to new regulatory mandates, such as new requirements for International Automated Clearing House Transactions.

The system scans each transaction looking for signs of fraud and identifies suspicious or high-risk transactions based on established criteria. If fraud is detected, the system alerts analysts, who place the transaction on hold until a representative can confirm whether the transaction is legitimate or fraudulent. If fraud is detected, the company refunds the money to the sender.

According to Bridenstine, IBM® InfoSphere® Identity Insight solutions are a cornerstone of the system, analyzing transaction data and enterprise data sources to determine whether individuals really are who they say they are. The software can search, analyze, and compare multicultural name data sets using culture-specific name data and linguistic rules and provide likely variations to reduce false negatives and false positives.

“InfoSphere Identity Insight provides the mechanism to move to a much more customer-centric view,” says Bridenstine.



“We’ve already stopped more than US\$37.7 million in fraudulent transactions and prevented thousands of customers from losing funds to fraud.”

— Ted Bridenstine

Once accurate identity is established, the system can determine whether people are, or ever have been, related in any way and apply complex event processing to evaluate all transactions of the entity and of associated entities. The rules engine also provides the business logic to alert staff when a transaction or the aggregation of a specific customer’s transactions exceeds a specific threshold.

Additionally, the solution gives MoneyGram the ability to respond quickly to new and different kinds of frauds. For instance, in 2010, MoneyGram noticed that fraudsters were receiving transactions in California. In early November 2010, MoneyGram analysts added a rule to the system that flagged transactions above a certain dollar amount sent to California. That simple change prevented US\$1.7 million in suspected fraudulent transactions in just three months. “We can now react within hours or minutes, changing rules or implementing new rules, if an analyst identifies a new pattern of behavior,” says Bridenstine.

This new flexibility is helping the company increase customer satisfaction and stay a step ahead of fraudsters. Consumer complaints of fraud in January 2011 compared to January 2010 dropped 72 percent, with the most significant reductions in Canada, Nigeria, the United States, and the United Kingdom. From February 2010 to January 2011, the anti-fraud technology accounted for a 40 percent increase in MoneyGram’s ability to identify and interrupt potentially fraudulent transactions.

“We are able to detect and respond to fraud faster than before to protect our consumers as well as our global network of agents,” says Bridenstine. “We must remain ever vigilant in the face of more sophisticated financial fraudsters. The solution stopped US\$30,000 of fraudulent transactions on the first day and within 17 days of operation, it had stopped US\$1 million of fraudulent transactions. We’ve already stopped more than US\$37.7 million in all in fraudulent transactions and prevented thousands of customers from losing funds to fraud.”



“InfoSphere Identity Insight provides the mechanism to accurately identify who our customers are and help us move to a much more customer-centric view.”

— Ted Bridenstine

► The inside story: Getting there

Offsite summit sets direction... According to Bridenstine, a multiday, offsite brainstorming and design session, which included application architects, business analysts and business stakeholders, was critical in identifying project requirements and possible solutions. During the summit, MoneyGram's CIO invited IBM to demonstrate its InfoSphere Identity Insight solution. “The CIO had seen a demonstration of IBM Software in Europe and felt that the solution might be of value in our discussions,” says Bridenstine. “During the demonstration, IBM showed how the software could resolve customer names and entities, even with complex ethnic variations.”

Following the successful summit, planning discussions ensued with IBM Business Partner Alpine Consulting and key MoneyGram subject matter experts. IBM proposed marrying its Complex Event Processing (CEP) functionality with InfoSphere Identity Insight software to afford an integrated and sophisticated rules engine to trigger system responses based on transaction behavior for a resolved entity (person).

A rudimentary set of requirements based on initial guidelines was developed and additional discussions with MoneyGram executives worldwide were conducted to gain clarity regarding data and regulatory requirements. Once the platform was solidified, Alpine Consulting delivered a two-month onsite proof-of-functionality to verify core functionality, identify any gaps, and help staff finalize project plans and budget.

Expanding beyond fraud... MoneyGram initially called its Global Compliance initiative the “Global Aggregation Project” based on the requirements of the Payment Services Directive. However, as business leaders reviewed the capabilities of IBM InfoSphere Identity Insight software, they recognized that the solution was flexible enough to address more than just the aggregation requirements.

“By using InfoSphere Identity Insight to build a single source for name resolution, we can create synergies between fraud, anti-money laundering, loyalty and possibly even watch list interdiction,” says Bridenstine.

For more information

To learn more about how IBM can help you transform your business, please contact your IBM sales representative or IBM Business Partner.

Visit us at: ibm.com/software/data/infosphere/identity-insight

For more information about MoneyGram International, visit:
www.moneygram.com

For more information about IBM Business Partner Alpine Consulting, Inc., visit: www.alpineinc.com



© Copyright IBM Corporation 2011

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2011
All Rights Reserved

IBM, the IBM logo, ibm.com, Let's build a smarter planet, smarter planet, the planet icons and InfoSphere are trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.



Please Recycle